学校编码：10384　　分类号_____　密级_____

学号：X2010230440　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

VPN 技术在企业信息化中的应用及研究

Application and Research of VPN Technology in Enterprise Informatization

香承凯

指导教师姓名：陈海山 教授

专 业 名 称 ：软 件 工 程

论文提交日期：2012 年 10 月

论文答辩时间：2012 年 11 月

学位授予日期：　　年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2012 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范(试行)》。

另外，本学位论文为(　　)课题(组)的研究成果，获得(　　)课题(组)经费或实验室的资助，在(　　)实验室完成(请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明)。

声明人(签名)：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文(包括纸质版和电子版)，允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

(　　)1.经厦门大学保密委员会审查核定的保密学位论文，于

年　月　日解密，解密后适用上述授权。

(　√　)2.不保密，适用上述授权。

(请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。)

声明人(签名)：

年　　月　　日

摘要

在互联网技术和通信技术迅猛发展的同时，VPN(Virtual Private Network)技术得到了迅速发展，其在网络中应用领域也不断扩大，并在使用中不断出现新的技术要求。VPN 作为网络应用层的一种远程访问技术，不仅基于成熟的互联网应用层协议，而且满足了大多数网络用户的需求，近年在企业信息化网络中得到了广泛应用。

VPN 作为一种新型的网络安全接入技术，处在不断的应用和完善阶段，因此也难免存在缺陷和不足(系统性能和终端安全方面)，需要在实际应用中加以改善。因此，对 VPN 技术的研究具有重要的现实意义。

根据所参与的新疆移动网络安全项目研究，从 VPN 技术协议入手，分析了四种 VPN 技术方案，并在相关关键技术上加以介绍，同时分析了企业信息化建设中遇到的问题。主要工作如下：

1.分析 VPN 及 SSL VPN 的技术，详细讨论了 VPN 的四种关键技术，并着重对 IPsec VPN、SSL VPN 安全性进行分析，主要对其存在的缺点以及急需改进之处作了论证分析。

2.结合国内企业信息化建设的现状，分析目前信息化建设中存在的问题，并根据用户需求的不同提出了相应的合理化建议。

3.结合新疆移动 VPN 业务部署情况以及乌鲁木齐市城域网中的 VPN 技术在当地企业信息化应用项目中的具体案例分析，研究了在 VPN 技术和传输城域网的综合应用中最终方案的设计和选定并予以实施的相关环节，包括组网技术分析、组网方案设计等相关内容。

关键词：VPN 技术；企业信息化；SSL VPN

Abstract

With the rapid development of internet and communication technology, VPN (Virtual Private Network) technology is developing rapidly; their application in the network has also been expanding; and emerging new technical requirements constantly. VPN (Virtual Private Network), as a new type of remote access technology of the network application layer, has many advantages due to its mature based protocol. It meets the needs of many users，and has been applied in the corporations increasingly in recent years.

VPN, as a new network security technology, is in a continuous application and improvement stage. Inevitably it has some defects and deficiencies which need to be improved in practical applications, such as system performance and endpoint security gaps. Therefore, there is important practical significance to study VPN.

Based on the participation of XinJiang CMCC network security projects, starting from the VPN technology agreement, four types of VPN technology program, and related key technologies to be introduced, while analysis of the problems encountered in the construction of enterprise information. The main work is as follows:

1. Introduced the concept of VPN and SSL VPN, describe the four key technologies of VPN in detail, and focus on the analysis of VPN security, mainly to discuss its shortcomings, and make needed improvements and analysis.

2. Combined with the current situation and the domestic construction of enterprise information, analysis of information construction, the rationalization proposals, depending on the user needs.

3. Combined of XinJiang CMCC VPN service deployment Urumqi VPN technology in local enterprise information application projects specific case studies, study design and selected the final program in the comprehensive application of the of VPN technology transfer MAN given and the implementation of related links, and including networking technology analysis, network design and other related content.

Keywords： VPN; Enterprise Information; SSL VPN

目录

Contents

第1章 绪论

1.1 论文选题的背景及意义

随着信息时代的来临，企业的发展也日益呈现出产业多元化、结构分布化、管理信息化的特征。计算机网络技术不断提升，信息管理范围不断扩大，不论是企业内部职能部门，还是企业外部的供应商、分支机构和外出人员，都需要同企业总部之间建立起一个快速、安全、稳定的网络通信环境。怎样建立外部网络环境与内部网络环境之间的安全通信，实现企业外部分支机构远程访问内部网络资源，成为当前很多企业在信息网络化建设方面亟待解决的问题。

随着互联网技术和电子商务的蓬勃发展，基于 Internet 的商务应用在企业信息管理领域得到了长足发展。根据企业的商务活动，需要一些固定的生意伙伴、供应商、客户也能够访问本企业的局域网，从而简化信息传递的路径，加快信息交换的速度，提高企业的市场响应速度和决策速度。同时，围绕企业自身的发展战略，企业的分支机构越来越多，企业需要与各分支机构之间建立起信息相互访问的渠道。面对越来越复杂的网络应用和日益突出的信息处理问题，VPN 技术无疑给我们提供了一个很好的解决思路。

VPN 可以帮助远程用户同公司的内部网建立可信的安全连接，并保证数据的安全传输，通过将数据流转移到低成本的网络上，大幅度地减少了企业、分支机构、供应商和客户花在信息传递环节的时间，降低了企业局域网和 Internet 安全对接的成本。VPN 的应用建立在一个全开放的 Internet 环境之中，这样就大大简化了网络的设计和管理，满足了不断增长的移动用户和 Internet 用户的接入，以实现安全快捷的网络连接。

1.2 论文的主要工作

企业信息化建设的长期性和复杂性使得企业内部网络的改进并不能一蹴而

就，而是要持续进行的，在系统建设及应用推广过程中，需要针对不同重要程度的业务应用以及内部数据的重要程度，制定相应的用户访问权限量及业务接入标准。企业信息化的建设及质量的改进也不是单个部门就可以完成，它需要项目的所有开发部门、实施部门和开发人员协调、通力合作。论文根据 VPN 技术的特点、企业信息化项目的实施经验以及通过对目前主流 VPN 技术原理的分析，从安全性、简便性及可实施性三个方面比较，通过分析目前企业信息化网络现状的难题和需求，探讨了用 VPN 技术构建企业内部网的优势所在，并详细地研究了 IPSec VPN、SSL VPN、MPLS VPN 三种不同组网技术的原理以及各自优缺点。通过对主流 VPN 技术研究后，结合新疆移动 VPN 业务部署情况以及乌鲁木齐市城域网中的 VPN 技术在当地企业信息化应用项目中的具体案例分析，研究了在 VPN 技术和传输城域网的综合应用中最终方案的设计和选定并予以实施的相关环节，研究内容包括组网技术分析、组网方案设计等。

组建 VPN 网络的总体目标是在保证安全性、稳定性的基础上综合考虑可扩展性、易于管理以及经济性等方面，用尽量少的投资满足用户当前以及可预计的未来的需求。

1.3 国内外研究现状

虚拟专用网 VPN 技术的研究开始于 20 世纪 90 年代，目前实现 VPN 常用的技术包括配置管理技术、隧道技术、协议封装技术和密码技术等。这些技术可应用于 TCP/IP 协议中的数据链路层、IP 层、TCP 层和应用层。目前较为成熟的 VPN 实用技术均有相应的协议规范和配置管理方法。根据实现技术的不同，VPN 主要可分为 L2TP(Layer2 Tunneling Protocol)、L2F (Layer2 Forwarding)、MPLS(Multi Protocol Label Switch)、IPSec(IP Security)、SSL(Secure Sockets Layer)等几类。其中，IPSec VPN 和 SSL VPN 是目前应用最广泛的两种 VPN 解决方案。

IPSecVPN 是一种出现较早、较为成熟的 VPN 技术。其通过实现 IPSec 协议族，提供安全性服务：数据加密、完整性校验、数据源身份认证、访问控制。工作在网络层的 IPSec VPN 能担负大数据量传输的任务，但其安装配置非常繁琐，不易灵活部署在复杂网络环境中，特别是在远程访问控制方面。

SSL VPN 是近年来兴起的一种新型安全 VPN，它是一种基于隧道技术，利用 SSL/TLS 协议结合强加密算法、身份认证技术开发而成的安全 VPN。它通过数据包封装技术来实现虚拟专用网的私有性，通过 PKI 技术和加密技术来鉴别通信双方的身份和确保传输数据的安全。SSL VPN 工作在网络应用层，具有组网灵活性强、管理维护成本低、用户操作简便等特点。SSL VPN 支持 IPv4/v6、Netware IPX、AppleTalk 等多种网络协议，可成功穿越 NAT 设备。由于 SSL VPN 是支持 Web 访问无客户端或瘦客户端组件的，与 IPSecVPN 相比，更符合越来越多的移动式、分布式办公的需求。

SSL VPN 的优势主要体现在以下几个方面：无需安装客户端软件；适用于大多数设备；适用于大多数操作系统；良好的安全性；较强的资源控制能力；减少费用；可以绕过防火墙和代理服务器进行访问。

随着 SSL VPN 应用的逐渐升温，越来越多的企业开始采纳 SSL VPN 的网络架构，来解决企业的远程访问需求。许多国际网络安全厂商正在对 SSL VPN 这种新型业务进行重点投资，如 Cisco、Nokia、Juniper、Symantec 等在内的国际知名厂商。

国内的 VPN 市场从 2000 年正式起步，由金融、政府、通信等行业带动起步，到今天，国内也有不少相关产品研制成功并得以应用，如深圳深信服公司的 M5X00-S 系列、上海冰峰公司的 ICEFLOW S 系列等的产品均得到了广泛的应用。国内的研究成果主要集中在 SSL VPN 网关上，使用 SSL 代理，即在 SSL 网关和用户之间建立 SSL 连接，实现数据全程加密；采用双 SSL 网关技术，增加企业 VPN 系统的可靠性。

1.4 论文的组织结架

论文共分五章，各章内容如下：

第一章是引言，主要介绍了论文的研究背景和研究现状，简述论文的主要研究内容。

第二章介绍了企业信息化应用系统在建设过程中所涉及的网络基础理论，并对 VPN 技术的概念、技术组成和关键技术做了简单介绍。

第三章详细分析了 VPN 技术的 L2TP(Layer2 Tunneling Protocol)、MPLS(Multi Protocol Label Switch)、IPSec(IP Security)、SSL(Secure Sockets Layer)技术原理及相对应的网络解决方案，着重分析了目前广泛应用的 SSL VPN 解决方案，详细分析了 SSL VPN 的四个关键技术，最后对 SSL VPN 的安全性进行了分析。

第四章本文作者结合新疆移动 VPN 业务部署情况以及乌鲁木齐市城域网中的 VPN 技术在当地企业信息化应用项目中的具体案例分析，研究了在 VPN 技术和传输城域网的综合应用中最终方案的设计和选定并予以实施的相关环节，包括组网技术分析、组网方案设计等相关内容。

第五章在总结论文工作的基础上，阐述论文工作的不足与今后的努力方向。

第2章 网络基础理论

现代意义上的计算机网络是从 1969 年美国国防部高级研究计划局建成的 ARPAnet 实验网开始的。当时只有 4 个结点，发展到现在的正如其名所言如蜘蛛网一般的复杂的互联网。威胁与安全一直都是并存着的。窃听、假冒、重放、拒绝服务、病毒、诽谤等等的威胁无时无刻攻击着网络通信，威胁着我们的信息安全。然而提供这些威胁存在的原因正是由于操作系统、计算机网络、数据库管理系统存在着本身的漏洞，这就使得一些非法授权的行为可以“祸起萧墙”。专家把这些可能使得一个网络受到破坏的所有行为都认定为攻击，它可以是主动攻击、被动攻击、物理临近攻击、内部人员攻击和分发攻击，所有的一切都威胁着网络的安全。

Internet 的安全话题一直以来都是发散而复杂的。从最初把 Internet 作为科学研究用途，到当今的电子商务炙手可热之时，安全已然成为网络发展的绊脚石。所以有更多的安全技术顺势而出，目前的安全措施有数据加密、数字签名、身份认证、防火墙和内容检查等。这些虽然不能阻止风险的出现，但可以把风险降到最低。

专用网络指的是企业内部的局域和广域网络，是 Internet 等公共网络上的延伸。在过去，大型企业为了网络通讯的需求，往往必须投资人力、物力及财力，来建立企业专用的广域网络通讯管道，或采用长途电话甚至国际电话的昂贵拨接方式。在 Internet 蓬勃发展的现在，企业为了维持竞争力，又为了使公司总部和分支、合作伙伴之间信息的安全性受到保障，通常需要将专用网络与 Internet 间适当地整合在一起，但是又必须花费一笔 Internet 连接的固定费用。基本上 Internet 是建立在公众网络的基础之上，如果企业可以将专用网络中的广域网络连结与远程拨号连接这两部份，架构在 Internet 这一类的公众网络之上，同时又可以维持原有的功能与安全需求的话，则将可以节省下一笔不算小的通讯费用支出。

2.1 网络通信技术

网络通讯技术(NCT:Network Communication Technology)是指通过计算机和网

络通讯设备对图形和文字等形式的资料进行采集、存储、处理和传输等，使信息资源达到充分共享的技术。通信网是一种由通信端点、节(结)点和传输链路相互有机地连接起来，以实现在两个或更多的规定通信端点之间提供连接或非连接传输的通信体系。

通信网按功能与用途不同，一般可分为物理网、业务网和支撑管理网等三种。物理网是由用户终端、交换系统、传输系统等通信设备所组成的实体结构，是通信网的物质基础，也称装备网。用户终端是通信网的外围设备，它将用户发送的各种形式的信息转变为电磁信号送入通信网路传送，或将从通信网路中接收到的电磁信号等转变为用户可识别的信息。用户终端按其功能不同，可分为电话终端、非话终端及多媒体通信终端。电话终端指普通电话机、移动电话机等；非话终端指电报终端，传真终端、计算机终端、数据终端等；多媒体通信终端指可提供至少包含两种类型信息媒体或功能的终端设备，如可视电话、电视会议系统等。交换系统是各种信息的集散中心，是实现信息交换的关键环节。传输系统是信息传递的通道，它将用户终端与交换系统之间以及交换系统相互之间联接起来，形成网路。传输系统按传输媒介的不同，可分为有线传输系统和无线传输系统两类。有线传输系统以电磁波沿某种有形媒质的传播来实现信号的传递。无线传输系统则是以电磁波在空中的传播来实现信号的传递。

业务网是疏通电话、电报、传真、数据、图像等各类通信业务的网路，是指通信网的服务功能。按其业务种类，可分为电话网、电报网，数据网等。电话网是各种业务的基础，电报网是通过在电话电路加装电报复用设备而形成的，数据网可由传输数据信号的电话电路或专用电路构成。业务网具有等级结构，即在业务中设立不同层次的交换中心，并根据业务流量、流向、技术及经济分析，在交换机之间以一定的方式相互联接。

支撑管理网是为保证业务网正常运行，增强网路功能，提高全网服务质量而形成的网络。在支撑管理网中传递的是相应的控制、监测及信令等信号。按其功能不同，可分为信令网、同步网和管理网。信令网由信令点、信令转接点、信令链路等组成，旨在为公共信道信令系统的使用者传送信令。同步网为通信网内所有通信设备的时钟(或载波)提供同步控制信号，使它们工作在同一速率(或频率)上。管理网是为保持通信网正常运行和服务所建立的软、硬系统，通常可分为话务管理网和传输

监控网两部分。

2.2 网络信息安全技术

理解信息安全的概念有利于人们更容易地了解各种名目繁多及众多延伸出来的信息安全理论及其方法技术。

一般认为安全的信息具有如下三个特点：

1.信息的完整性(Integrity)

信息在存储、传递和提取的过程中没有残缺、丢失等现象的出现，这就要求信息的存储介质、存储方式、传播媒体、传播方法、读取方式等要完全可靠，因为信息总是以一定的方式来记录、传递与提取的，它以多种多样的形式存储于多样的物理介质中，并随时可能通过某种方式来传递。简单地说如果一段记录由于某种原因而残缺不全了，那么其记录的信息也就不完整了。那么我们就可以认为这种存储方式或传递方式是不安全的。

2.信息的机密性(Confidentiality)

简单理解就是信息不被泄露或窃取。人们总希望有些信息不被自己不信任的人所知晓，因而采用一些方法来防止，比如把秘密的信息进行加密，把秘密的文件放在别人无法拿到的地方等等，都是实现信息机密性的方法。

3.信息的有效性(Availability)

一种是对信息的存取有效性的保证，即以规定的方法能够准确无误地存取特定的信息资源；一种是信息的时效性，指信息在特定的时间段内能被有权存取该信息的主体所存取。等等。但信息安全概念是随着时代的发展而发展的，信息安全概念以及内涵都在不断地发展变化，并且人们以自身不同的出发点和侧重点不同提出了许许多多不同的理论。另外，针对某特定的安全应用时，这些关于信息安全的概念也许并不能完全地包含所有情况，比如信息的真实性(Authenticity)、实用性(Utinity)、占有性(Possession)等，就是一些其他具体的信息安全要求而提出的。

网络信息安全所要解决的问题：

计算机网络安全的层次上大致可分为：物理安全、安全控制、安全服务三个方面。